09/555305
526 Rec'd PCT/PTO 26 MAY 2000
15.05.2000

Encoding method for carrying out cryptographic operations.

Technical field

The invention relates to an encryption method as disclosed in the introductory part of Claim 1 wherein at least one cryptographic sub-operation $y_i = f_i(x_i,k_i)$ is performed on data x_i, k_i which are digitally stored as data bit words, the relevant result or intermediate results y_i being digitally stored or buffered as data bit words. The invention also relates to an encryption device as disclosed in the introductory part of Claim 8 which includes a processor and registers R_i, the processor performing at least one cryptographic sub-operation $y_i = f_i(x_i,k_i)$ on operands x_i, k_i which are digitally stored as data bit words in the registers R_i of the encryption device, the relevant result or intermediate results y_i being digitally stored or buffered as data bit words in the registers R_i of the encryption device.

State of the art

Cryptographic operations are carried out in many data processing apparatus so as to protect the operation of such apparatus or the data transported in the apparatus. The arithmetic operations required for this purpose are carried by standard processors as well as by dedicated crypto processors. A typical example of the latter processor is formed by a chip card or an IC card. As is shown in Fig. 1, for such cryptographic calculations it is often necessary to initialize relevant storage sections or registers of the data processing apparatus with operands x_i, k_i. During the i^{th} calculation intermediate results y_i are possibly stored in storage sections or registers R_i or subsequently the result of the calculation is stored in storage sections or registers for further processing. The register R_i is situated between a preceding i^{th} cryptographic calculation and a subsequent $(i+1)^{th}$ cryptographic operation. The data x_i, k_i or intermediate results y_i used in this context customarily constitute security-relevant information such as, for example, cryptographic keys or operands.

In order to calculate the cryptographic algorithms the data processing apparatus form logic combinations of operands k_i or intermediate results y_i or x_i, x_{i+1}. Depending on the technology used, such operations, notably the loading of the storage sections or registers with data, lead to an increased current consumption of the data processing apparatus. In the case of complementary logic, for example CMOS, an increase of

the current consumption occurs when the value of a bit storage cell changes, i.e. when its value changes from "0" to "1" or from "1" to "0". The increase of the consumption is then dependent on the number of bit positions changed in the memory or register. In other words, the loading of a previously erased register causes an increase of the current consumption which is proportional to the Hamming weight of the operand (= number of bits having the value "1") or to the difference in the Hamming weight. Analysis of such a current variation could thus enable extraction of information concerning the operations executed, thus enabling successful crypto analysis of secret operands such as, for example, cryptographic keys. For example, in the case of very small signal variations, adequate information could be extracted by carrying out a plurality of current measurements on the data processing apparatus. On the other hand, a plurality of measurements could also enable a possibly required differentiation. This type of crypto analysis is also called "Differential Power Analysis" whereby an outsider could successfully perform a possibly unauthorized crypto analysis of the cryptographic operations, algorithms, operands or data purely by observing changes in the current consumption of the data processing apparatus.

From US 5,297,201 it is known to combine a high frequency radiating computer with a device which also radiates high frequency similar to that of the computer. As a result, unauthorized third parties can no longer decode the high-frequency radiated by the computer. This system, however, cannot prevent crypto analysis by a third party having direct access to the computer.

In order to eliminate a correlation in chip cards between the output of a result of a cryptographic operation or a transfer of key information for a cryptographic operation and the cryptographic operation itself, it is known from Patent Abstracts of Japan 10069222A to delay the result of the cryptographic operation or the transfer of the key information for the cryptographic operations. However, this system can also be analyzed by way of Differential Power Analysis, because the delayed data transfer also becomes apparent in the current consumption of the data processing apparatus.

Implementation of the invention, object, solution, advantages

It is an object of the present invention to provide an improved method and an improved device of the kind set forth which eliminate the described drawbacks and effectively prevent crypto analysis by observation of current consumption of a data processing apparatus.

This object is achieved by a method of the kind set forth which is characterized as disclosed in Claim 1.

To this end, according to the invention at option at least one of the data x_i, k_i and/or the result or at least one intermediate result y_i is bit-wise complemented to $\bar{y} = f(\bar{x}_i, \bar{k}_i)$ and/or $\bar{y}_i$ or not, depending on a control signal r_i which is based on random numbers.

This offers the advantage that other bit series are processed or stored in the case of repeated execution of the same cryptographic operation, so that the respective execution of a cryptographic operation or several cryptographic operations produce different current variations in the data processing apparatus. Irrespective of the actual value of the sub-results, in the case of repeated execution of the overall calculation it is thus achieved that each data path changes the same number of times from "0" to "0", from "0" "1", from "1" to "0" and from "1" to "1" in the case of a pure random number series or practically the same number of times in the case of a pseudo-random number series. However, because the control signal r_i based on random numbers is not known or predetermined, there will be no correlation between the current variations and the bit values of the data and results, so that Differential Power Analysis no longer leads to successful crypto analysis. In other words, the mean current consumption of the overall operation does not contain usable information concerning the sub-operands or intermediate results used in the sub-operations.

Advantageous further versions of the method are disclosed in the Claims 2 to 7.

Preferably, one or more XOR combinations (EXCLUSIVE- OR combinations) are formed during the cryptographic sub-operations.

The data contain, for example cryptographic keys and/or operands.

In a preferred version intermediate results y_i are buffered in a register R_i between the execution of successive cryptographic sub-operations and are used as an operand x_{i+1} for the subsequent cryptographic sub-operations.

In order to form an original, non-inverted value after each sub-operation, a bit series $x_{i+1} = y_i$ derived from the intermediate result y_i of a preceding sub-operation i is bit-wise complemented to $\bar{x}_{i+1}$ for a subsequent sub-operation i+1 if the data x_i, k_i of the preceding sub-operation i were bit-wise complemented.

In a particularly advantageous version at least one bit value, notably the even bit values, the odd bit values or all bit values, of a data bit word x_i, k_i or y_i are inverted during the bit-wise complementary operation. It is then particularly advantageous to perform an

inversion of bit values or bit addresses of a data bit word x_i, k_i or y_i by means of an XOR operation (EXCLUSIVE-OR operation) during the bit-wise complementary operation.

A device of the kind set forth according to the invention is provided with at least one inverter which can be controlled by a control signal r_i and serves for at least one of the data x_i, k_i and/or the result or at least one intermediate result y_i, with a random number generator which generates random numbers, as well as with a device for generating the control signal r_i on the basis of the random numbers, the controllable inverter either, in dependence on the control signal r_i, converting the bit series x_i, k_i or y_i into their bit-wise complement $\bar{x}_i$, $\bar{k}_i$ and $\bar{y}_i$, respectively, or leaving them unchanged.

This offers the advantage that other bit sequences are processed or stored in the case of repeated execution of the same cryptographic operation, so that other current variations occur in the data processing apparatus during the respective execution of the cryptographic operation or cryptographic operations. Irrespective of the actual value of the sub-results, in the case of repeated execution of the overall calculation it is thus achieved that each data path changes the same number of times from "0" to "0", from "0" to "1", from "1" to "0" and from "1" to "1" in the case of a pure random number series or practically the same number of times in the case of a pseudo-random number series. However, because the control signal r_i based on random numbers is not known or predetermined, there will be no correlation between the current variations and the bit values of the data and results, so that Differential Power Analysis no longer leads to successful crypto analysis. In other words, the mean current consumption of the overall operation does not contain usable information concerning the sub-operands or intermediate results used in the sub-operations.

Advantageous further embodiments of the device are described in the Claims 9 to 14.

In a preferred embodiment at least one register R_i is succeeded by an inverter which receives the same control signal r_i as the inverter for the data x_i, k_i which precedes the i^{th} sub-operation. The inverter succeeding a register R_i of the i^{th} sub-operation is preferably combined with an inverter for input data x_{i+1} which precedes the subsequent $(i+1)^{th}$ sub-operation. The combined inverter preferably receives the control signal r_i of the preceding i^{th} sub-operation as well as the control signal r_{i+1} of the subsequent $(i+1)^{th}$ sub-operation.

The data contain, for example, cryptographic keys and/or operands.

In a preferred embodiment a register R_i stores an intermediate result y_i of the preceding i^{th} sub-operation between a preceding i^{th} sub-operation and a subsequent $(i+1)^{th}$

sub-operation and forwards this intermediate result as an input value x_{i+1} to the subsequent $(i+1)^{th}$ sub-operation.

Preferably, the bit-wise complementary operation inverts at least one bit value, notably the even bit values, the odd bit values or all bit values, of a data bit word x_i, k_i or y_i.

Brief description of the drawings

The invention will be described in detail hereinafter with reference to the accompanying drawings. Therein:

Fig. 1 shows a flow chart of a part of a cryptographic operation according to the state of the art,

Fig. 2 shows a flow chart of a part of a first preferred version of a cryptographic operation according to the invention, and

Fig. 3 shows a flow chart of a part of a second preferred version of a cryptographic operation according to the invention.

Preferred implementation of the invention

In the first preferred version of an encryption method according to the invention as shown in Fig. 2 a cryptographic overall operation is performed by way of a chain of sub-operations $f_i(x_i,k_i)$ in which one or more logic XOR (EXCLUSIVE OR) combinations are formed. The Figure shows two sub-operations, i.e. the i^{th} sub-operation 10 and the $(i+1)^{th}$ sub-operation 12, each sub-operation being executed by an arithmetic unit. Each sub-operation 10, 12 is succeeded by a storage cell or a register R_i 14 and a storage cell or a register R_i 16, respectively. Each sub-operation 10, 12 has as its input value data x_i, x_{i+1} as well as an operand k_i, k_{i+1}, both being available as data bit words.

Each sub-operation 10, 12 is preceded by a respective controllable inverter 18 and 20 for the data x_i, x_{i+1}, respectively, as well as by a controllable inverter 22, 24 for the operands k_i, k_{i+1}. Furthermore, for each sub-operation 10, 12 the relevant register R_i 14 and R_{i+1} 16 is succeeded by a controllable inverter 26, 28 for the intermediate result y_i, y_{i+1}, said intermediate result being propagated by the relevant register R_i 14 and R_{i+1} 16 to a subsequent sub-operation 12 as input data x_{i+1} and x_{i+1}, respectively. The inverters 18 to 28 can be controlled by a control signal r_i and r_{i+1}, respectively, in such a manner that at option they bit-wise complement the associated data bit words or not, depending on the relevant control signal r_i and r_{i+1}, respectively. All inverters 18, 22, 26 and 20, 24, 28 of a sub-operation 10 and 12, respectively, then receive the same control signal r_i and r_{i+1},

respectively. In other words, the decision whether an inversion of the relevant input values of the inverters 18 to 28 is performed or whether the input values traverse the inverters 18 to 28 in non-processed form is taken by the additional control signal r_i and r_{i+1}, respectively. This arrangement of registers 14, 16 between sub-operations 10, 12 is used particularly when the sub-operations 10, 12 are calculated successively in time by one and the same unit so that the sub-results must be buffered.

The control signal is controlled by random values from a random generator in such a manner that, depending on the value of the random numbers, the sub-operation yields either the original result y = f(x,k) or the bit-inverted result $\bar{y} = \bar{f}(\bar{x}, \bar{k})$. It is thus achieved that the calculation as well as the storage of the data in the registers R_i 14, 16 takes place either by way of original values or bit-inverted values. In the case of repeated execution of the overall calculation it is thus achieved that each data path changes over the same number of times from "0" to "0", from "0" to "1", from "1" to "0" and from "1" to "1", irrespective of the actual value of the sub-results. The mean current consumption of the overall operation, consequently, does not contain useful information concerning the sub-operands k_i or intermediate results y_i involved in the sub-operations 10, 12. The inverter 26, 28 succeeding the registers 14, 16 restores the original, non-inverted value again for the next sub-operation 12 again.

The second preferred version of the encryption method according to the invention as shown in Fig. 3 corresponds to the first version shown in Fig. 2, the only difference being that the inverters 26, 28 succeeding the registers 14, 16 are combined with the respective input inverter 20 of the next stage 12 so as to form an inverter 30.

The inverters invert, for example, only a part of the bit values of the relevant data bit word. For example, only the even or the odd bit words or bit addresses are inverted. The bit values are inverted, for example, by means of an XOR (EXCLUSIVE OR) operation.

09553005.052500